UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/715,350	11/17/2000	David Montgomery	0500.0003231	6328

23418 7590 05/26/2006

VEDDER PRICE KAUFMAN & KAMMHOLZ
222 N. LASALLE STREET
CHICAGO, IL 60601

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 05/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/715,350	MONTGOMERY, DAVID	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,12-17,19-21,24-33,35 and 37-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *39* is/are allowed.

6)☒ Claim(s) *1,2,4-7,12-17,19-21,24-33,35,37,38 and 40-46* is/are rejected.

7)☒ Claim(s) *3* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 3/9/2006 was received and considered.

2. Claims 1-7, 12-17, 19-21, 24-33, 35, 37-46 are pending.

3. Claim 39 is allowable.

4. Claim 3 is objected to.

Response to Arguments

5. Applicant's arguments filed 3/9/2006 have been fully considered but they are not persuasive.

6. Applicant's response (p. 14) makes the statement that the office action does not provide a rejection for Applicant's claims, for example claim 12. However, a rejection was supplied for claim 12 in §16 of the Office Action. Further, applicant addresses the rejection of claim 12 on p. 15 of applicant's response.

7. Applicant's response (p. 14) suggests that a typographical error in claim 1 has been corrected. However the corrected is not reflected in the submitted claims. Therefore, the objection is maintained.

8. Applicant's amendment overcomes the rejection of claim 15 under 35 U.S.C. §112.

9. Applicant's response (p. 14) argues that (1) the term "signed certificate set" includes a set of certificate related data that is signed and that (2) the signed certificate set cannot contain zero entries. Applicant also makes the statement that "In any event, the claims have been amended to address the office action's comments". Therefore, in light of Applicant's amendments, the signed certificate set is understood to mean a set of certificate related data over which a digital

signature is created and in which the digital signature is included and the rejection of claims 1-7, 12-17, 19-21, 24-33, 35 & 37-45 is withdrawn. It is noted that claim 46 has not been amended and, therefore, the rejection is maintained.

10. Applicant's response (p. 15) argues that the rejection of claims 16-17, 19-21, 24-29 & 38-44 under 35 U.S.C. §101 is inappropriate in view of the Patent Office guidelines and since there is no basis for this rejection. Applicant cites the fact that claim 16 is directed to an apparatus and is not directed to software, per se. However, Applicant is directed to p. 11, ¶2 of the specification where the following is recited: "Each signed certificate set generate 104a-104n, may be a server or, for example, a software application, discrete logic, a plurality of processing units, or any other suitable structure that is operative to collect a plurality of cross certificates...". Applicant is further directed to p. 10, ¶3 of the specification where the following is recited: "In this example, the client units 106a-106n may be, for example, but are not limited to, software applications, or any suitable processing unit that contains, for example, a cryptographic engine ...". Therefore, for example, while claim 16 recites an apparatus, the elements of the "apparatus", when read in light of the specification, suggest the claimed apparatus may be software, per se. Similarly, claim 26 recites a system comprising a signed certificate set generator and at least one client unit, both of which can be software. Similarly, claims 42-44 recites an apparatus comprising a signed certificate generator, which may be software. Further, claims 26-38 & 40-44 do not produce a tangible result, but rather manipulate data. Therefore, the rejection of claims 16-17, 19-21, 24-29, 38 & 40-44. The rejection of claim 39 under 35 U.S.C. §101 is withdrawn, as the step of "publishing" produces a tangible result.

11. Applicant's response (p. 15) argues that "Applicant is unable to find any mention of a cross certificate in the cited portion. However, Menezes is relied upon for teaching cross certificates.

12. Applicant's response (p. 16) argues that there is no teaching of enterprise administrator cross certificates in Samar or Menezes and no motivation provided by the mere definition of a cross certificate. However, Samar teaches an enterprise administrator collecting a set of certificates that the administrator determines should be trusted by the owner of the wallet (obtaining at least on public key and identifier) (col. 5, lines 53-57) and creating a signed certificate set/signed certificate list identifying a plurality of units/CA's determined to be trusted by the anchor/enterprise manager, wherein the set includes certificates (each having a public key and identifier) and an associated digital signature/fingerprint (col. 6, lines 14-46). Samar is silent regarding how the determines what CA's the owner of the wallet is expected to trust, and hence is silent regarding the use of a cross certificate. However, Menezes teaches that a cross certificate is a certificate created by one certification authority to certify another CA (p. 572). This motivation to combine is proper because one of ordinary skill in the art would be motivated to use an existing cross certificate, which according to Menezes are known in the art, rather than separately verify certificate authorities. Therefore, it is maintained that one of ordinary skill in the art would be motivated to modify Samar, when determining trusted CA's (for inclusion in Samar's wallet), in accordance with the teaching of Menezes to cause the enterprise administrator to access one of it's own cross certificates (certifying another CA). One of ordinary skill in the art would have been motivated to perform such a modification because this is the exact use of cross certificates, according to Menezes and trusted CA's must be identified in

Samar's invention. Further, Applicant amends, for example, claim 1 to include such that the signed certificate set includes an associated digital signature. As Samar's list of certificates is signed, it contains an associated digital signature (associated with the signed certificate set).

Claim Objections

13. Claim 1 is objected to because of the following informalities: "trusted certificate issuing unit" (last line) should be replaced with "trusted certificate issuing units". Appropriate correction is required.

Claim Rejections - 35 USC § 112

14. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

15. Claims 46 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 1-7, 12-17, 19-21, 24-33, 35, 37-45, it is unclear if the "associated digital signature" is associated with the public key, unique identifier, trusted certificate issuing units or the signed certificate set. *For the purposes of this Office Action, the digital signature is understood to be associated with (created over) the signed certificate set.*

Regarding claim 46, "signed certificate set" can be interpreted as equivalent to "a set of certificates that is signed" or "a set of signed certificates" and the claims are therefore vague and indefinite.

Claim Rejections - 35 USC § 101

16. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

17. Claims 16-17, 19-21, 24-29, 38 & 40-44 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed to subject matter not necessarily carried out using a computer or an apparatus containing software, per se (see pp. 10-11 of the instant specification).

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. Claims 1-2, 4-7, 12-17, 19-21, 24-33, 35, 37-38, 40-41, 43 & 45-46, as best understood, are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,304,974 to **Samar**, in view of Handbook of Applied Cryptography, by Menezes et al. (**Menezes**).

Regarding claims 1, 4, 6-7, 12, 14, 16, 19-21, 24, 26, 29-30, 32-33, 35, 41 & 46, Samar discloses for a community of interest, collecting at least one cross certificate/list of certificates (col. 6, lines 14-21) associated with another anchor certificate issuing unit/enterprise administrator, and obtaining at least one certificate issuing unit/ trusted certificate authority (col.

6, lines 14-21) public key and associated identifier for a cross-certified certificate issuing unit/trusted certificate authority identified by the at least one cross certificate (col. 6, lines 28-34) and creating a signed certificate set (col. 6, lines 28-34) identifying a plurality of certificate issuing units/certificate authorities determined to be trusted by the anchor certificate issuing unit/enterprise administrator based on the at least one cross certificate/list of certificates, wherein the signed certificate set includes at least the unique identifier and the public key (certificate) of each of the plurality of trusted certificate issuing units (col. 6, line 24 – col. 7, line 16) and an associated digital signature/signed certificate set (col. 6, lines 40-46). Samar lacks explicitly collecting cross certificates in creating the signed certificate set. However, Menezes teaches that a cross-certificate is a certificate created by one certification authority to certify the public key of another (p. 572, 13.39 Definition). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Samar to collect the enterprise administrator's cross-certificates to build the list of trusted CA's for use in the wallet. One of ordinary skill in the art would have been motivated to perform such a modification because a cross-certificate is a certificate created by one certification authority to certify the public key of another, as taught by Menezes (p. 572, 13.39 Definition).

Regarding claims 2, 17, 27-28 & 31, Samar, as modified above, lacks generating a signed certificate set revocation list. However, Menezes teaches that a certificate revocation list is a signed list of revoked public keys (certificates), including an identifier of the associated certificate (p. 577) when a CA loses trust in a particular public key (p. 576, §13.6.3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a signed certificate set revocation list containing at least an identifier of at least

one signed certificate set that has been revoked. One of ordinary skill in the art would have been motivated to perform such a modification to prevent subsequent use of or trust in a certificate, as taught by Menezes (pp. 576-577).

Regarding claims 5 & 37, Samar, as modified above, lacks explicitly requests by one or more clients. However, the examiner takes Official Notice that a client requesting a service is old and well established in the art of the user/administrator model as a method of servicing a client through an administrator. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Samar's enterprise administrator to further accept request from a client for the certificate list. One of ordinary skill in the art would have been motivated to perform such a modification to service a client's need for a certificate list. This advantage is well known to those skilled in the art.

Regarding claims 13 & 25, Samar, as modified above, discloses identifying trusted certificate issuing units based on cross certificates and conveying that trust to clients, but lacks explicitly validating a digital signature associated with each cross certificate and only including certificate issuing units that had valid certificates. However, Menezes teaches that the purpose of certificates are to be validated to determine authenticity of a public key (p. 560, §13.23 (ii)) and to convey trust in that public key to another entity (definition 13.22). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to validate the digital signature on the trusted CA's certificates and only include valid certificates in the signed certificate set/list of trusted certificates. One of ordinary skill in the art would have been motivated to perform such a modification to only convey trust in valid certificates, as taught by Menezes (pp. 559-560).

Regarding claims 15, 38, 43 & 45, Samar, as modified above, lacks including identifiers of policy constraints in the signed certificate set. However, Menezes teaches that including expiration dates in certificates limits exposure following compromise (p. 577, #1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the certificate list of Samar to include a policy identifier/expiration date. One of ordinary skill in the art would have been motivated to perform such a modification to limit exposure following compromise, as taught by Menezes (p. 577, #1).

Regarding claim 40, Samar, as modified above, lacks adding assigned certificate set identifier associated with a given anchor certificate issuing unit. However, Menezes teaches that common forms of additional information are added to certificates, such as a serial number to identify the certificate (§13.4.2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a serial number in the signed certificate set. One of ordinary skill in the art would have been motivated to perform such a modification to identify the certificate set, as taught by Menezes (§13.4.2).

Allowable Subject Matter

20. Claim 3 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

21. Claim 39 is allowed.

22. The following is a statement of reasons for the indication of allowable subject matter:

a. Regarding claim 3, the prior art relied upon fails to teach or suggest the step of collecting at least one of the plurality of cross certificates including obtaining chained cross certificates from a plurality of certificate issuing units, in combination with the other limitations of the claim.

b. Regarding claim 39, the prior art relied upon fails to teach or suggest publishing a signed certificate set of certificate issuing units and determining, by a client unit if the signed certificate set of trusted certificate issuing units is revoked and whether the signed certificate set needs to be regenerated for the anchor certificate issuing unit, in combination with the other limitations of the claim.

Conclusion

23. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis Jacques can be reached at (571) 272-6962.

Any response to this action should be mailed to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-8300
(for formal communications intended for entry)
Or:
(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS

May 15, 2006

JACQUES H. LOUIS-JACQUES
PRIMARY EXAMINER